THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL. XV. DECEMBER, 1908. NO. 12.

ON THE FACTORIZATION OF LARGE NUMBERS.

By PROFESSOR L. E. DICKSON, Ph. D., The University of Chicago.

1. In the study of a difficult problem, it is a decided handicap to be denied the useful information that accompanies a knowledge of the origin of the proposed problem. There is little interest and much labor in the factorization of numbers taken at random. The real desideratum is a method which is capable of making effective use of the information which can be derived from the origin of the proposed number, and of auxiliary tables at command. For example, we may be concerned with numbers of a given form such as $m^n \pm 1$, or with the eliminant* of a system of congruences under investigation. We shall here illustrate such a method by determining the composition, hitherto unknown, of two numbers each of eleven digits. The first of these is a, where

$$A = \tfrac{1}{27}(26^{13}+1) = 937.6449.a, \quad a = 15207498827.$$

The first two prime factors were obtained by Lt. Col. Cunningham by means of his tables of solutions of $y^n \pm 1 \equiv 0 \pmod{q}$, for $n < 16$, q prime and $< 10^4$.

2. Let p be a prime factor of a. Applying Fermat's theorem, we have

$$26^{p-1} \equiv 1, \quad 26^{26} \equiv 1 \pmod{p},$$

so that $p-1$ is an even multiple of 13. Thus $p = 1 + 26n$. Now

$$a = 1 + 26N, \quad N = 584903801.$$

Let $a = pq$. Then $1 \equiv q \pmod{26}$, $q = 1 + 26n_1$. Then $a = pq$ gives

$$N = n + n_1 + 26nn_1. \tag{1}$$

*Instances of rapid factorizations of numbers known to be true eliminants occur in the writer's paper, "On the last theorem of Fermat," *Quarterly Journal of Mathematics*, Vol. 40 (1908), p. 40.

But $N \equiv 1 \pmod{26}$. Hence $n+n_1=1+26l$, l an integer. Then

$$nn_1+l=M\equiv 22496300.$$

If l were odd, n and n_1 would both be odd, whereas $n+n_1$ is odd. Thus $l=2t$. Then $(n_1-n)^2=(n_1+n)^2-4nn_1$ has the value

$$Q=(1+52t)^2-4(M-2t).$$

Thus Q must be a square. But $M\equiv 2$, $Q\equiv t^2+t-1 \pmod{3}$. If $t^2+t\equiv 0$, Q would be a quadratic non-residue of 3. Hence t is not congruent to $0, -1 \pmod{3}$. Thus $t=3k+1$,

$$Q=(156k+53)^2+24k+8-4M. \tag{2}$$

Since $1+26n>10^4$, $n\geqq 385$, $n_1\leqq 58490$. On the hyperbola (1), $n+n_1$ is a minimum when $n=n_1$, viz., for n approximately $474a$, since $\sqrt{a}$ just exceeds 123300. Thus $l\geqq 365$, $k\geqq 60$. For the above limits the maximum value of $n+n_1$ is approximately $385+58490$; hence $l\leqq 2264$, $k\leqq 377$.

We form the residues of Q modulo r, where r is one of the primes 5, ..., 23, and require that Q be a quadratic residue* of r. Thus

$$\begin{aligned}
&Q\equiv k^2+2,\ k\equiv \pm 2 \pmod{5};\\
&Q\equiv 4[(k-2)^2+1],\ k\equiv 1, 2, 3 \pmod{7};\\
&Q\equiv 4[(k+2)^2-3],\ k\equiv 0, 3, 4, 7, 8, 10 \pmod{11};\\
&Q\equiv -2k+3,\ k\equiv 0, 1, 2, 3, 6, 8, 10 \pmod{13};\\
&Q\equiv 9[(k+2)^2+1],\ k\equiv 2, 3, 5, 8, 10, 11, 14, 15, 16 \pmod{17};\\
&Q\equiv 16[(k-5)^2+6],\ k\equiv 4, 5, 6, 11, 12, 14, 15, 17, 18 \pmod{19};\\
&Q\equiv 25(k^2-6),\ k\equiv \pm 1, \pm 3, \pm 8, \pm 9, \pm 10, \pm 11 \pmod{23}.
\end{aligned}$$

From the results for $r=5$, $r=7$, and $60\leqq k\leqq 377$, we have

$$k=35x_1+2,\ 35x_2+3,\ 35x_3+8,\ 35x_4+17,\ 35x_5+22,\ 35x_6+23\ (2\leqq x_i\leqq 10).$$

Then, modulo 11, $\frac{1}{2}k\equiv x+1$, 7, 4, 3, 0, 6. But $\frac{1}{2}k\equiv 0, 2, 4, 5, 7, 9$. Thus†

$$\begin{aligned}
&x_1=3, 4, 6, 8, 10;\quad x_2=2, 4, 6, 8, 9;\quad x_3=3, 5, 7, 9;\\
&x_4=2, 4, 6, 8, 10;\quad x_5=2, 4, 5, 7, 9;\quad x_6=3, 5, 7, 9, 10.
\end{aligned}$$

Modulo 13, $3k\equiv x+6$, 9, 11, 12, 1, 4. But $3k\equiv 0, 3, 4, 5, 6, 9, 11$. Hence,

*These are given by the tables of indices in texts on the theory of numbers.

†The x_i are obtained by addition and suppressing positive residues other than 2, ..., 10.

$$x_1=3,\ 5,\ 7,\ 10;\quad x_2=2,\ 4,\ 7,\ 8,\ 9,\ 10;\quad x_3=2,\ 5,\ 6,\ 7,\ 8;$$
$$x_4=4,\ 5,\ 6,\ 7,\ 10;\quad x_5=2,\ 3,\ 4,\ 5,\ 8,\ 10;\quad x_6=2,\ 5,\ 7,\ 9.$$

For modulo 17, $35x_i\equiv x_i$. Hence

$$x_1=3,\ 6,\ 8,\ 9;\quad x_2=2,\ 5,\ 7,\ 8;\quad x_3=2,\ 3,\ 6,\ 7,\ 8;$$
$$x_4=2,\ 3,\ 5,\ 8,\ 10;\quad x_5=3,\ 5,\ 6,\ 9,\ 10;\quad x_6=2,\ 4,\ 5,\ 8,\ 9,\ 10.$$

The values of the x_i common to the three sets are

$$x_1=3;\quad x_2=2,\ 8;\quad x_2=7;\quad x_4=10;\quad x_5=5;\quad x_6=5,\ 9.$$

Modulus 19 excludes $x_2=2$, $k\equiv16$; $x_5=5$, $k\equiv7$; $x_6=5$, $k\equiv8$. Modulus 23 excludes $x_2=8$, $k\equiv7$; $x_3=7$, $k\equiv0$; $x_6=9$, $k\equiv-7$. Of the two remaining values,* $x_1=3$ gives $k=107$, $l=6k+2=644$, whence

$$Q=(13799)^2,\quad n_1-n=13799,\quad n_1+n=16745,\quad n_1=15272,$$
$$n=1473,\quad 1+26n=38299,\quad 1+26n_1=397073,$$

the two prime factors of a.

3. We next determine the composition of

$$b=31401724537=\frac{56^7-1}{56-1}=1+56N,\qquad N\equiv\frac{56^6-1}{56-1}.$$

By Fermat's theorem, a prime factor p of b has the form $14k+1$ and hence $56l+1$, $+15$, $+29$, $+43$. The second and third forms are excluded by Legendre's table of divisors of quadratic forms, or as follows. If $p=56l+15$, 2 is a quadratic residue of p, and 7 a non-residue, in view of the reciprocity law. Thus 14 is a non-residue of p, contrary to $56^8\equiv56 \pmod{p}$.

If $b=pq$, then $q\equiv1 \pmod{14}$, $q=1+14k_1$. Thus

$$k+k_1+14kk_1=4N=4.57(56^4+56^2+1).$$

Hence $k+k_1\equiv4 \pmod{14}$, so that

$$k+k_1=4+14h,\quad kk_1+h=16.57(56^3+56)+16. \tag{3}$$

First let $k=4l+3$, so that $p=56l+43$. By (3), $k_1+3\equiv2h$, $3k_1+h\equiv0 \pmod{4}$, whence $k_1\equiv h\equiv3 \pmod{4}$. Set $h=4t+3$, $k_1=4l_1+3$. Then by (3),

*For $x_4=10$, $k=367\equiv-10 \pmod{29}$, $Q\equiv3$, a quadratic non-residue of 29.

$$l+l_1=14t+10, \quad 4ll_1+43t=4.57(56^3+56)-29.$$

By the latter, $t\equiv 1(\text{mod. }4)$, $t=4c+1$. Hence

$$\tfrac{1}{4}(l_1-l)^2=S=16(7c+3)^2+43c+18-57(56^3+56).$$

Thus $S\equiv 3c+2(\text{mod. }8)$. If c is odd, $S\equiv 1$, $c\equiv 5(\text{mod. }8)$. If c is even, S must be a multiple of 4, whence $c\equiv 2(\text{mod. }4)$, $c=4m+2$, $\tfrac{1}{4}S\equiv 43m(\text{mod. }32)$. If m is odd, then $m\equiv 3(\text{mod. }8)$. If m is even, then $m=4r$, and $\tfrac{1}{16}S\equiv 3r$ (mod. 8), so that either r is a multiple of 4 or $r\equiv 3(\text{mod. }8)$. Hence we have the cases

$$(4) \qquad c\equiv 5(\text{mod. }8), \quad c=32w+14, \quad 64w+2, \quad 128w+50.$$

Modulo 81, S is the product of 16 by $S'=49c^2+70c+15$. In particular, $S'\equiv c^2+c(\text{mod. }3)$. Thus $c\equiv 0$ or 2(mod. 3). If c is a multiple of 3, S' must be a multiple of 9, so that $c=3+9d$, $S'\equiv 9(4d+2)$, mod. 81. Thus, $4d+2\equiv 0, 1, 4, 7(\text{mod. }9)$, $d\equiv 4, 2, 5, 8$. Next, if $c=2+3e$, $S'\equiv 6e(\text{mod. }9)$, $e=3f$. Thus $S'\equiv 9(5f+3)$, mod. 81, $f\equiv 2, 3, 5, 8(\text{mod. }9)$. Hence

$$(5) \qquad c\equiv 20, 21, 29, 39, 47, 48, 74, 75(\text{mod. }81).$$

$$S\equiv 4c^2+3,\ c\equiv \pm 2(\text{mod. }5); \quad S\equiv c+1,\ c\equiv 0, 1, 3, 6(\text{mod. }7);$$
$$S\equiv 16(5c^2+3),\ c\equiv 0, \pm 2, \pm 3(\text{mod. }11);$$
$$S\equiv 4(c^2+1),\ c\equiv 0, \pm 3, \pm 4, \pm 5(\text{mod. }13);$$
$$S\equiv 2[(c-4)^2-2],\ c\equiv 2, 3, 4, 5, 6, 10, 11, 14, 15(\text{mod. }17).$$

By the tables cited, b has no factor $<10^4$. Thus, $1+14k\geqq 9999$, $1+14k_1\leqq 3140172$. Hence $k\geqq 714$, $k_1<224298$, $l\geqq 178$, $l_1<56074$. The sum of the latter gives the maximum $l+l_1$. Thus $t<4018$, $c\leqq 1004$. Since $\sqrt{b}$ just exceeds 177205, the approximate value for equal k's just exceeds 12657. Thus the equal l's just exceed 3164. Hence $t\geqq 451$, $c>112$.

For the first case under (4), we set $c=81x+20, \ldots, 75$, by (5). Thus

$$5\equiv x+4, 5, 5, 7, 7, 0, 2, 3; \quad x\equiv 1, 0, 0, 6, 6, 5, 3. 2(\text{mod. }8).$$

The resulting values of c between 112 and 1005 are

525, 669, 749, 885, 965; 533, 237, 677; 453, 317.

The first five are excluded by mod. 5, the next three by mod. 11, the last two by mod. 7.

For $c=32w+14$, $4 \leqq w \leqq 30$ by the limits on c. By (5),

$$w \equiv 66, 23, 3, 59, 39, 77, 12, 50 (\text{mod. } 81),$$

respectively. Hence $w=23$, 12. But 23 is excluded mod. 5, and 12 mod. 17.

For $c=64w+2$, $2 \leqq w \leqq 15$. But $w \equiv 0, 4 (\text{mod. } 5)$, $w \equiv 0, 1, 2, 5, 8 (\text{mod. } 11)$. Hence $w=5$, $c=322 \equiv 79 (\text{mod. } 81)$, and is excluded by (5).

For $c=128w+50$, $1 \leqq w \leqq 7$. By (5), $w=3$, $c=434$, excluded mod. 5.

4. It remains to determine whether or not b has a factor $1+56n$. The complementary factor is of the form $1+56n_1$. Hence

$$n+n_1+56nn_1=N.$$

By inspection, $N \equiv 1 (\text{mod. } 56)$. Hence there is an integer l for which

$$n+n_1=56l+1, \quad nn_1+l=C=\frac{56^5-1}{56-1}=10013305,$$
$$(n_1-n)^2=S=(56l+1)^2+4l-4C.$$

Modulo 56, $S \equiv 4l-3$. Thus $S \equiv 1 (\text{mod. } 8)$, $l \equiv 1 (\text{mod. } 2)$, $l=2\lambda+1$. Also $S \equiv \lambda+1 (\text{mod. } 7)$, $\lambda \equiv 0, 1, 3, 6 (\text{mod. } 7)$. We have

$$S=112^2\lambda^2+8.1597\lambda-40049967.$$

Modulo 81, S is the product of $112^2 \equiv -11$ by $\sigma=\lambda^2+2\lambda+15$. The latter must be a quadratic residue of 81. In particular, $\lambda+1 \equiv \pm 1+3t$. Then $\sigma \equiv 6 \pm 6t (\text{mod. } 9)$; thus $\sigma \equiv 0 (\text{mod. } 9)$, $t \equiv \mp 1 (\text{mod, } 3)$, $\lambda+1=\mp 2+9f$. Then $\sigma \equiv 9(2 \mp 4f)$, mod. 81. Thus $2 \mp 4f$ is one of the quadratic residues 0, 1, 4, 7 of 9, whence $\pm f \equiv 5, 7, 4, 1 (\text{mod. } 9)$. Hence

$$\lambda \equiv 6, 19, 33, 37, 42, 46, 60, 73 (\text{mod. } 81).$$
$$4S \equiv (\lambda+2)^2-2, \quad \lambda \equiv 2, 4 (\text{mod. } 5);$$
$$S \equiv 4[(\lambda+2)^2+4], \quad \lambda \equiv 2, 5, 8, 9, 10 (\text{mod. } 11);$$
$$S \equiv 25[(\lambda-5)^2-3], \quad \lambda \equiv 0, 1, 3, 5, 7, 9, 10 (\text{mod. } 13);$$
$$8S \equiv (\lambda+2)^2-9, \quad \lambda \equiv \pm 1, -2, \pm 3, -5, 6, \pm 7 (\text{mod. } 17).$$

Since b has no factor $<10^4$, $n>178$, $n_1<56075$. The maximum $n+n_1$ is approximately 56253, whence $l<1005$, $\lambda<502$. The minimum $n+n_1$ is given by $n=n_1=3165-$. Hence $l \geqq 113$, $\lambda \geqq 56$. From the above residues moduli 81 and 5,

$$\lambda=405t+19, 37, 42, 87, 114, 127, 154, 199, 204, 222, 249, 262, 289, 357, 384, 397.$$

For the first three $t=1$; for the fourth $t=0$, 1; for the others $t=0$. Of the 17 resulting values of λ, 114, 222, 249, 289, 397, 424, 492 are excluded by mod. 7; then 127, 154, 199, 204, 447 are excluded by mod. 11; 262 and 357 by mod. 13; 87 and 442 by mod. 17; for the remaining value $\lambda=384$, $S\equiv 21$ (mod. 23), whereas 21 is a quadratic non-residue of 23.

Hence $b=\frac{1}{55}(56^7-1)$ *is a prime.*

While it is believed that the above work is accurate, having been carefully checked, it should be added that the same result was found by an earlier proof different as to details.

5. By the same method, I obtain the following results:

$$56^7+1=3.19.15737.1925393,$$
$$34^{17}+1=5.7.307.443.1531.28051.112643.4708729,$$
$$52^{13}+1=53.4057.21841.4328028093013,$$

all of the given factors being prime. That the last number of 13 digits is prime, I have verified by two proofs differing as to details. The factor 21841 was found by accident by Lt. Col. Cunningham. I ran across the factor 112643 of the second number in the manner explained in the *Quarterly Journal*, 1908, page 45; but the remaining two large factors were found by the present method.

6. In view of the interest in the numbers m^m-1 and their importance in connection with the last theorem of Fermat, it is desirable that some arithmetician should check the statement of E. Lucas (*American Journal of Mathematics*, Vol. 1, 1878, p. 294) that the large factors of 10 and 12 digits in $22^{11}\pm1$ are actually primes. For a verification by the present method it is of the greatest help to know that there are no factors less than 10,000, in view of the tables by Lt. Col. Cunningham. The latter believes that Lucas intended to record his factors as primes; but that an uncertainty runs right through his factorizations as to the primality of the factors, no clue whatever being given as to how the primality was detected.

FACTORING IN A DOMAIN OF RATIONALITY.

By ELIZABETH R. BENNETT, The Universtty of Illinois.

If a series of symbols R_1, R_2, ... which are supposed to obey the ordinary laws of algebra, but are not necessarily thought of as representing numbers, are combined with respect to the four fundamental operations of arithmetic—addition, subtraction, multiplication, and division, division by zero being excluded, there result a series of expressions which are rational